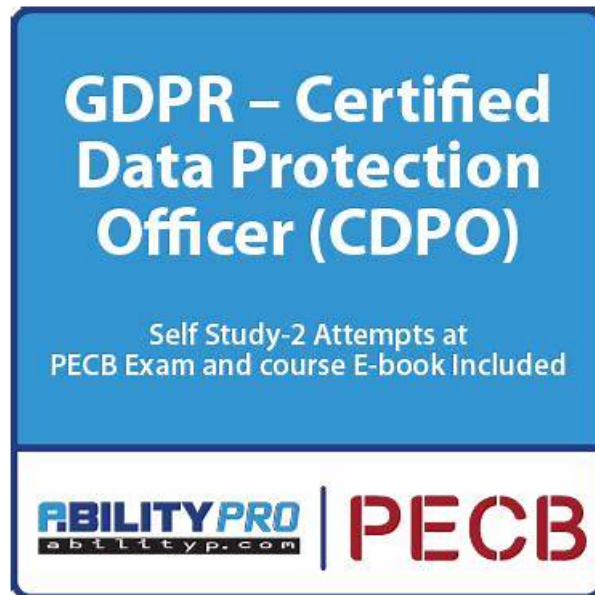


PECB Certified Data Protection Officer study guide & GDPR reliable questions & PECB Certified Data Protection Officer pdf dumps



P.S. Free 2025 PECB GDPR dumps are available on Google Drive shared by VCEdumps: <https://drive.google.com/open?id=1zfNMIMkVt4gfiRZZImOB9ma-0gCfzs5>

VCEdumps are responsible in every aspect. After your purchase our GDPR practice braindumps, the after sales services are considerate as well. We have considerate after sales services with genial staff. They are willing to solve the problems of our GDPR Exam Questions 24/7 all the time. About the dynamic change of our GDPR study guide, they will send the updates to your mailbox according to the trend of the exam.

Our PECB GDPR desktop and web-based practice software are embedded with mock exams, just like the actual PECB Data Center certification exam. The VCEdumps designs its mock papers so smartly that you can easily prepare for the PECB Certified Data Protection Officer exam. All the essential questions are included, which have a huge chance of appearing in the real PECB Certified Data Protection Officer exam. Our mock exams may be customized so that you can change the topics and timings for each exam according to your preparation.

>> GDPR Valid Test Practice <<

GDPR Hottest Certification, GDPR New Real Test

All these GDPR certification exam benefits will not only prove your skills but also assist you to put your career on the right track and achieve your career objectives in a short time period. These are all the advantages of the PECB Certified Data Protection Officer (GDPR) certification exam. To avail of all these advantages you just need to enroll in the PECB exam dumps and pass it with good scores. To pass the GDPR exam you can get help from VCEdumps PECB Questions easily.

PECB GDPR Exam Syllabus Topics:

Topic	Details

Topic 1	<ul style="list-style-type: none"> Roles and responsibilities of accountable parties for GDPR compliance: This section of the exam measures the skills of Compliance Managers and covers the responsibilities of various stakeholders, such as data controllers, data processors, and supervisory authorities, in ensuring GDPR compliance. It assesses knowledge of accountability frameworks, documentation requirements, and reporting obligations necessary to maintain compliance with regulatory standards.
Topic 2	<ul style="list-style-type: none"> This section of the exam measures the skills of Data Protection Officers and covers fundamental concepts of data protection, key principles of GDPR, and the legal framework governing data privacy. It evaluates the understanding of compliance measures required to meet regulatory standards, including data processing principles, consent management, and individuals' rights under GDPR.
Topic 3	<ul style="list-style-type: none"> Technical and organizational measures for data protection: This section of the exam measures the skills of IT Security Specialists and covers the implementation of technical and organizational safeguards to protect personal data. It evaluates the ability to apply encryption, pseudonymization, and access controls, as well as the establishment of security policies, risk assessments, and incident response plans to enhance data protection and mitigate risks.
Topic 4	<ul style="list-style-type: none"> Data protection concepts: General Data Protection Regulation (GDPR), and compliance measures

PECB Certified Data Protection Officer Sample Questions (Q80-Q85):

NEW QUESTION # 80

Scenario:

ChatBubble is a software company that stores personal data, including usernames, emails, and passwords.

Last month, an attacker gained access to ChatBubble's system, but the personal data was encrypted, preventing unauthorized access.

Question:

Should the data subjects be notified in this case?

- A. Yes, but only if the supervisory authority explicitly requests notification.
- B. Yes, the company shall communicate all incidents regarding personal data to the data subjects.
- C. No, the company is not required to notify data subjects about a data breach that affects a large number of individuals.
- D. No, the company is not required to notify data subjects when the personal data is protected with appropriate technical and organizational measures.

Answer: D

Explanation:

Under Article 34(3)(a) of GDPR, if personal data is encrypted or otherwise protected, notification to data subjects is not required unless the risk is high.

- * Option C is correct because encryption renders the data unintelligible to unauthorized parties, reducing risk.
- * Option A is incorrect because not all breaches require data subject notification—only those posing high risks.
- * Option B is incorrect because the number of affected individuals does not determine notification requirements.
- * Option D is incorrect because notification is based on risk assessment, not supervisory authority requests alone.

References:

- * GDPR Article 34(3)(a) (No notification required if encryption makes data inaccessible)
- * Recital 86 (Notification is necessary only if data loss poses a significant risk)

NEW QUESTION # 81

Scenario 4:

Berc is a pharmaceutical company headquartered in Paris, France, known for developing inexpensive improved healthcare products. They want to expand to developing life-saving treatments. Berc has been engaged in many medical researches and clinical trials over the years. These projects required the processing of large amounts of data, including personal information. Since 2019, Berc has pursued GDPR compliance to regulate data processing activities and ensure data protection. Berc aims to positively impact human health through the use of technology and the power of collaboration. They recently have created an innovative solution in participation with Unty, a pharmaceutical company located in Switzerland. They want to enable patients to identify signs of strokes or other health-related issues themselves. They wanted to create a medical wrist device that continuously monitors patients' heart rate and notifies them about irregular heartbeats. The first step of the project was to collect information from individuals aged

between 50 and 65. The purpose and means of processing were determined by both companies. The information collected included age, sex, ethnicity, medical history, and current medical status. Other information included names, dates of birth, and contact details. However, the individuals, who were mostly Berc's and Unty's customers, were not aware that there was an arrangement between Berc and Unty and that both companies have access to their personal data and share it between them. Berc outsourced the marketing of their new product to an international marketing company located in a country that had not adopted the adequacy decision from the EU commission. However, since they offered a good marketing campaign, following the DPO's advice, Berc contracted it. The marketing campaign included advertisement through telephone, emails, and social media. Berc requested that Berc's and Unty's clients be first informed about the product. They shared the contact details of clients with the marketing company. Based on this scenario, answer the following question:

Question:

Based on scenario 4, Berc followed the DPO's advice for outsourcing an international marketing company in the absence of an adequacy decision. Is the DPO responsible for evaluating this case?

- A. No, the controller or processor should evaluate cases when the adequacy decision is absent.
- B. No, because the marketing company operates under the same data protection rules as Berc.
- C. Yes, the DPO takes the final decision on transferring personal data to an international company in the absence of an adequacy decision.
- D. Yes, the DPO should evaluate cases where an adequacy decision is absent.

Answer: A

Explanation:

Under Article 44 of GDPR, the controller (Berc) is responsible for ensuring lawful data transfers. The DPO advises on compliance but does not make final decisions on data transfers.

* Option C is correct because the controller (Berc) must evaluate the legality of the transfer.

* Option A is incorrect because DPOs provide advice but do not evaluate data transfer legality.

* Option B is incorrect because DPOs do not have executive decision-making authority.

* Option D is incorrect because data protection rules vary by jurisdiction, making this assumption incorrect.

References:

* GDPR Article 44 (General principle for transfers)

* GDPR Article 39(1)(a) (DPO's advisory role)

NEW QUESTION # 82

Scenario 5:

Repond is a German employment recruiting company. Their services are delivered globally and include consulting and staffing solutions. In the beginning, Repond provided its services through an office in Germany. Today, they have grown to become one of the largest recruiting agencies, providing employment to more than 500,000 people around the world. Repond receives most applications through its website. Job searchers are required to provide the job title and location. Then, a list of job opportunities is provided. When a job position is selected, candidates are required to provide their contact details and professional work experience records. During the process, they are informed that the information will be used only for the purposes and period determined by Repond. Repond's experts analyze candidates' profiles and applications and choose the candidates that are suitable for the job position. The list of the selected candidates is then delivered to Repond's clients, who proceed with the recruitment process. Files of candidates that are not selected are stored in Repond's databases, including the personal data of candidates who withdraw the consent on which the processing was based. When the GDPR came into force, the company was unprepared.

The top management appointed a DPO and consulted him for all data protection issues. The DPO, on the other hand, reported the progress of all data protection activities to the top management. Considering the level of sensitivity of the personal data processed by Repond, the DPO did not have direct access to the personal data of all clients, unless the top management deemed it necessary. The DPO planned the GDPR implementation by initially analyzing the applicable GDPR requirements. Repond, on the other hand, initiated a risk assessment to understand the risks associated with processing operations. The risk assessment was conducted based on common risks that employment recruiting companies face. After analyzing different risk scenarios, the level of risk was determined and evaluated. The results were presented to the DPO, who then decided to analyze only the risks that have a greater impact on the company. The DPO concluded that the cost required for treating most of the identified risks was higher than simply accepting them. Based on this analysis, the DPO decided to accept the actual level of the identified risks. After reviewing policies and procedures of the company, Repond established a new data protection policy. As proposed by the DPO, the information security policy was also updated. These changes were then communicated to all employees of Repond. Based on this scenario, answer the following question:

Question:

Based on scenario 5, the DPO reports directly to Repond's top management. Is this in alignment with GDPR requirements?

- A. No, DPOs should report directly to department heads, not top management.

- B. Yes, based on GDPR, the controller may choose any reporting structure for the DPO, including top and middle management.
- **C. Yes, Article 38 of the GDPR requires that the DPO reports directly to the highest management level of the controller.**
- D. No, Article 38 of the GDPR requires that the DPO reports directly to the supervisory authority to ensure independence in performing their tasks.

Answer: C

Explanation:

Under Article 38(3) of GDPR, the DPO must report directly to the highest level of management to ensure independence and avoid interference in their tasks.

* Option A is correct because GDPR requires direct reporting to top management.

* Option B is incorrect because the DPO does not report to the supervisory authority, but they can liaise with it.

* Option C is incorrect because GDPR does not allow reporting to middle management.

* Option D is incorrect because department heads cannot oversee the DPO's work, ensuring they remain free from conflict of interest.

References:

* GDPR Article 38(3) (DPO must report to highest management)

* Recital 97 (DPO's independence and protection from undue influence)

NEW QUESTION # 83

Scenario: 2

Soyled is a retail company that sells a wide range of electronic products from top European brands. It primarily sells its products in its online platforms (which include customer reviews and ratings), despite using physical stores since 2015. Soyled's website and mobile app are used by millions of customers. Soyled has employed various solutions to create a customer-focused ecosystem and facilitate growth. Soyled uses customer relationship management (CRM) software to analyze user data and administer the interaction with customers. The software allows the company to store customer information, identify sales opportunities, and manage marketing campaigns. It automatically obtains information about each user's IP address and web browser cookies. Soyled also uses the software to collect behavioral data, such as users' repeated actions and mouse movement information. Customers must create an account to buy from Soyled's online platforms. To do so, they fill out a standard sign-up form of three mandatory boxes (name, surname, email address) and a non-mandatory one (phone number). When the user clicks the email address box, a pop-up message appears as follows: 'Soyled needs your email address to grant you access to your account and contact you about any changes related to your account and our website. For further information, please read our privacy policy.' When the user clicks the phone number box, the following message appears: 'Soyled may use your phone number to provide text updates on the order status. The phone number may also be used by the shipping courier.' Once the personal data is provided, customers create a username and password, which are used to access Soyled's website or app. When customers want to make a purchase, they are also required to provide their bank account details. When the user finally creates the account, the following message appears: 'Soyled collects only the personal data it needs for the following purposes: processing orders, managing accounts, and personalizing customers' experience. The collected data is shared with our network and used for marketing purposes.' Soyled uses personal data to promote sales and its brand. If a user decides to close the account, the personal data is still used for marketing purposes only. Last month, the company received an email from John, a customer, claiming that his personal data was being used for purposes other than those specified by the company. According to the email, Soyled was using the data for direct marketing purposes. John requested details on how his personal data was collected, stored, and processed. Based on this scenario, answer the following question:

Question:

When completing the sign-up form, the user gets a notification about the purpose for which Soyled collects their email address. Is Soyled required by the GDPR to do so?

- A. No, Soyled should provide this information only when requested by users.
- **B. Yes, users must be informed of the purpose of collecting their personal data.**
- C. No, Soyled only needs to inform users about how their data is collected, stored, or processed.
- D. Yes, but only if the email is used for communication purposes beyond account creation.

Answer: B

Explanation:

Under Article 13 of GDPR, controllers must inform data subjects at the time of data collection about the purpose of processing their personal data. This ensures transparency and accountability.

Soyled provides a pop-up message explaining why the email is collected, which aligns with GDPR's transparency principles. Option A is correct. Option B is incorrect because GDPR requires notification at collection, not upon request. Option C is incorrect as GDPR mandates disclosure of purpose, not just storage and processing methods. Option D is misleading because the purpose must be disclosed regardless of communication intent.

References:

- * GDPR Article 13(1)(c)(Obligation to inform data subjects about processing purposes)
- * Recital 60(Transparency and accountability in data collection)

NEW QUESTION # 84

Bus Spot is one of the largest bus operators in Spain. The company operates in local transport and bus rental since 2009. The success of Bus Spot can be attributed to the digitization of the bus ticketing system, through which clients can easily book tickets and stay up to date on any changes to their arrival or departure time. In recent years, due to the large number of passengers transported daily, Bus Spot has dealt with different incidents including vandalism, assaults on staff, and fraudulent injury claims. Considering the severity of these incidents, the need for having strong security measures had become crucial. Last month, the company decided to install a CCTV system across its network of buses. This security measure was taken to monitor the behavior of the company's employees and passengers, enabling crime prevention and ensuring safety and security. Following this decision, Bus Spot initiated a data protection impact assessment (DPIA). The outcome of each step of the DPIA was documented as follows: Step 1: In all 150 buses, two CCTV cameras will be installed. Only individuals authorized by Bus Spot will have access to the information generated by the CCTV system. CCTV cameras capture images only when the Bus Spot's buses are being used. The CCTV cameras will record images and sound. The information is transmitted to a video recorder and stored for 20 days. In case of incidents, CCTV recordings may be stored for more than 40 days and disclosed to a law enforcement body. Data collected through the CCTV system will be processed by another organization. The purpose of processing this type of information is to increase the security and safety of individuals and prevent criminal activity. Step 2: All employees of Bus Spot were informed for the installation of a CCTV system. As the data controller, Bus Spot will have the ultimate responsibility to conduct the DPIA. Appointing a DPO at that point was deemed unnecessary. However, the data processor's suggestions regarding the CCTV installation were taken into account. Step 3: Risk Likelihood (Unlikely, Possible, Likely) Severity (Moderate, Severe, Critical) Overall risk (Low, Medium, High) There is a risk that the principle of lawfulness, fairness, and transparency will be compromised since individuals might not be aware of the CCTV location and its field of view. Likely Moderate Low There is a risk that the principle of integrity and confidentiality may be compromised in case the CCTV system is not monitored and controlled with adequate security measures. Possible Severe Medium There is a risk related to the right of individuals to be informed regarding the installation of CCTV cameras. Possible Moderate Low Step 4: Bus Spot will provide appropriate training to individuals that have access to the information generated by the CCTV system. In addition, it will ensure that the employees of the data processor are trained as well. In each entrance of the bus, a sign for the use of CCTV will be displayed. The sign will be visible and readable by all passengers. It will show other details such as the purpose of its use, the identity of Bus Spot, and its contact number in case there are any queries. Only two employees of Bus Spot will be authorized to access the CCTV system. They will continuously monitor it and report any unusual behavior of bus drivers or passengers to Bus Spot. The requests of individuals that are subject to a criminal activity for accessing the CCTV images will be evaluated only for a limited period of time. If the access is allowed, the CCTV images will be exported by the CCTV system to an appropriate file format. Bus Spot will use a file encryption software to encrypt data before transferring onto another file format. Step 5: Bus Spot's top management has evaluated the DPIA results for the processing of data through CCTV system. The actions suggested to address the identified risks have been approved and will be implemented based on best practices. This DPIA involves the analysis of the risks and impacts in only a group of buses located in the capital of Spain. Therefore, the DPIA will be reconducted for each of Bus Spot's buses in Spain before installing the CCTV system. Based on this scenario, answer the following question:

Question:

Is a DPIA necessary for Bus Spot?

- A. No, because the installation of a CCTV system in Bus Spot's buses does not involve processing of data that is likely to result in a high risk to the rights and freedoms of data subjects.
- B. No, because CCTV cameras used for security reasons are automatically exempt from GDPR requirements.
- **C. Yes, because the installation of a CCTV system in Bus Spot's buses involves systematic monitoring of a large number of individuals.**
- D. Yes, because the installation of a CCTV system in Bus Spot's buses involves a systematic and extensive evaluation of personal aspects relating to natural persons based on automated processing.

Answer: C

Explanation:

Under Article 35(3)(c) of GDPR, a DPIA is required when a large-scale systematic monitoring of public spaces is conducted. CCTV cameras in public transportation capture many individuals, making a DPIA mandatory.

- * Option A is correct because CCTV monitoring in public spaces is considered high-risk processing.
- * Option B is incorrect because CCTV processing does not involve automated decision-making or profiling.
- * Option C is incorrect because CCTV processing affects a large number of individuals, posing potential risks.
- * Option D is incorrect because security cameras are subject to GDPR unless used for purely household purposes (Recital 18).

References:

* Recital 91(Use of DPIA in video surveillance)

• • • • •

GDPR Hottest Certification: <https://www.vcedumps.com/GDPR-examcollection.html>

- P.S. Free & New GDPR dumps are available on Google Drive shared by VCEdumps: <https://drive.google.com/open?id=1zfNMIMkVt4gfrRZZImOB9ma-0gCfzts5>